DFIR Review

Chromebook Forensic Acquisition

Daniel Dickerman

Published on: May 26, 2020

Synopsis

Forensic question: How can data be recovered from a Chromebook device?	DFIR REVIEW - DFRWS METHODOLOGY DFIR REVIEW - DFRWS
OS: ChromeOS	DFIR REVIEW - DFRWS VALIDATED DFIR REVIEW - DFRWS
Tools: Three 32GB USB flash drives, Custom bash scripts (provided as an attachment), An additional USB drive where the bash scripts will be located, A large capacity USB hard drive large enough to hold a clone of the Chromebook/Chromebox internal hard drive, Chrome Browser, Chromebook Recovery Utility app, and the “Special” build of Chromium	

Procedures and scripts written by Special Agent Daniel Dickerman
Technical Advisor – IRS Criminal Investigation – Electronic Crimes
daniel dot dickerman at ci dot irs dot gov

THE PROCEDURES AND SCRIPTS IN THIS DOCUMENT ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR

About this document

This document is provided to the general Computer Forensic community as a starting point to incite further research by others in the community, with the goal of further refining these procedures and developing additional procedures. This document contains three main sections. The first section explains the importance of obtaining all available cloud data from Google either via legal process or via consent through the Google self-service “Takeout” mechanism. The second section provides scripts and instructions on capturing a decrypted logical backup of all encrypted data on a Chromebook/Chromebox if you have the username(s) and password(s) for the accounts on the Chromebook/Chromebox. The final section provides scripts and instructions on capturing a full physical disk clone of a Chromebook/Chromebox in some very limited situations. Please see each section for complete details.

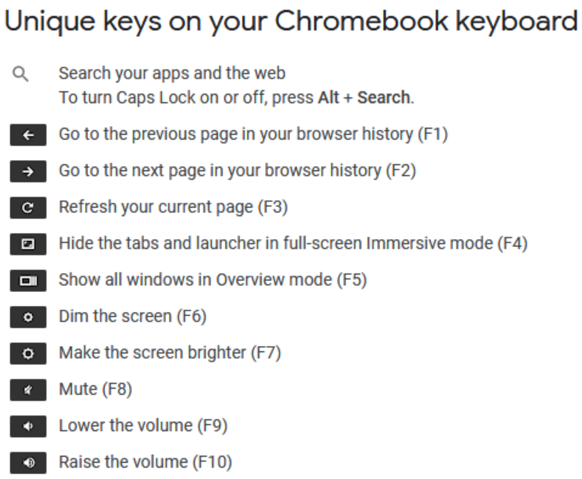
Since the public release of the previous revision of this document (v1.2), significant feedback has been provided by forensic examiners around the world. Additionally, further research, testing and tool development has taken place and is therefore included in this v1.3 revision.

Only the text and information in this v1.3 revision of the paper have been updated. No changes have been made to the scripts that perform the processes described in this paper and therefore the v1.2 scripts are still the most up-to-date scripts at the time of this writing.

General Information

Chromebook keyboard keys

Your Chromebook or Pixelbook does not have traditional keyboard keys and do not include Function (Fn) keys across the top of the keyboard. To use Fn keys on a Chromebook or Pixelbook, such as is needed to enter or switch between one of the virtual terminals (TTY1, TTY2, etc.) in either ChromeOS, Chromium OS or other, use the below links to identify the appropriate keyboard keys you need to press.



Unique keys on your Chromebook keyboard

Search your apps and the web
To turn Caps Lock on or off, press **Alt** + **Search**.

← Go to the previous page in your browser history (F1)

→ Go to the next page in your browser history (F2)

Refresh your current page (F3)

Hide the tabs and launcher in full-screen Immersive mode (F4)

Show all windows in Overview mode (F5)

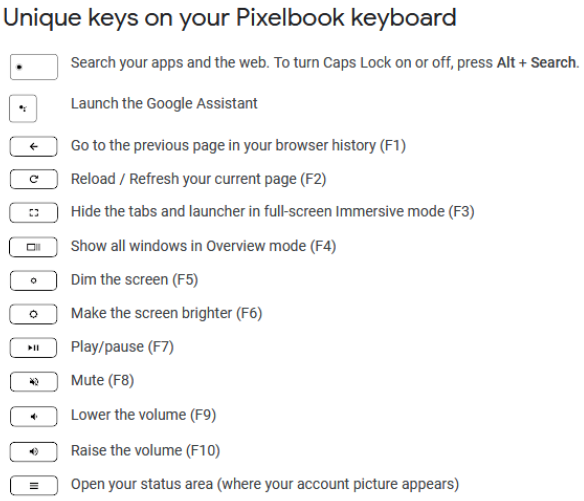
Dim the screen (F6)

Make the screen brighter (F7)

Mute (F8)

Lower the volume (F9)

Raise the volume (F10)



Unique keys on your Pixelbook keyboard

Search your apps and the web. To turn Caps Lock on or off, press **Alt** + **Search**.

Launch the Google Assistant

← Go to the previous page in your browser history (F1)

Reload / Refresh your current page (F2)

Hide the tabs and launcher in full-screen Immersive mode (F3)

Show all windows in Overview mode (F4)

Dim the screen (F5)

Make the screen brighter (F6)

Play/pause (F7)

Mute (F8)

Lower the volume (F9)

Raise the volume (F10)

≡ Open your status area (where your account picture appears)

The below links provide details about the keys found on most Chromebooks and the new Pixelbooks.

Use your Chromebook keyboard: https://support.google.com/chromebook/answer/1047364

Chromebook Keyboard shortcuts: https://support.google.com/chromebook/answer/183101

Use the Pixelbook keyboard: https://support.google.com/pixelbook/answer/7504061

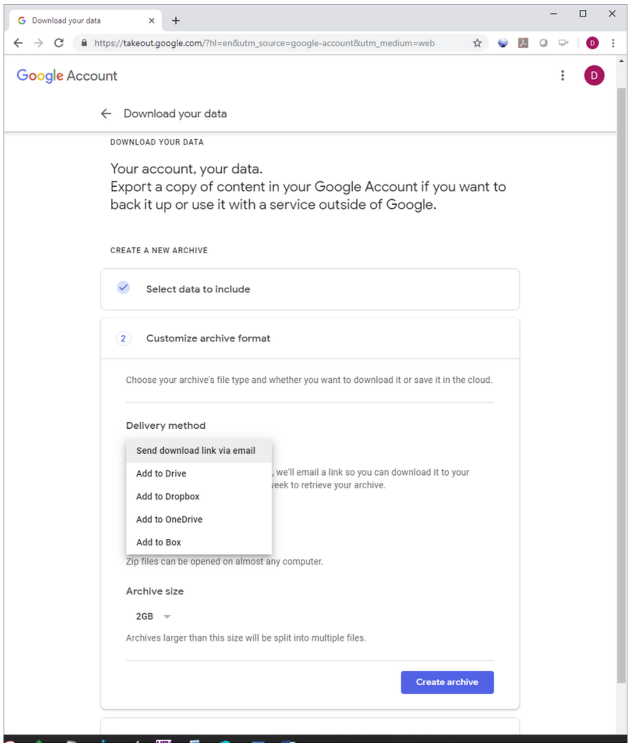
Pixelbook keyboard shortcuts: https://support.google.com/pixelbook/answer/7503852

Debug Button Shortcuts
https://chromium.googlesource.com/chromiumos/docs/+/master/debug_buttons.md

Obtaining Cloud Data

Chromebook and Chromebox devices are cloud-centric devices designed to be used via a live Internet connection in conjunction with Google Accounts. Depending on Privacy Settings for each Google Account, a significant amount of user data, to include: Personal Info; Account Security Info; People & Sharing Info (Contacts and Family Group info); Payments & Subscription Info; Activity History and Timeline (by location) for Web & App Activity, Location History, Voice & Audio Activity, Device Information, YouTube Search History; and activity and stored content from Google Services you use (i.e. Account, AdWords, Android, Books, Google Calendar, Chrome, Contacts, Google Drive, Gmail, Google Play Store, Google+, Google Payments and YouTube).

If you have a cooperating owner of a Google Account, the owner may provide online access to their Google Account and allow the export of a complete copy of all data in the Google Account via Google Takeout. https://takeout.google.com/?hl=en&utm_source=google-account&utm_medium=web


Download your data
https://takeout.google.com/?hl=en&utm_source=google-account&utm_medium=web
Google Account
D

Download your data

DOWNLOAD YOUR DATA

Your account, your data.
Export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

CREATE A NEW ARCHIVE

✓ Select data to include

2 Customize archive format

Choose your archive's file type and whether you want to download it or save it in the cloud.

Delivery method

Send download link via email
Add to Drive
Add to Dropbox
Add to OneDrive
Add to Box

, we'll email a link so you can download it to your
/eek to retrieve your archive.

Zip files can be opened on almost any computer.

Archive size

2GB

Archives larger than this size will be split into multiple files.

Create archive

If you do not have a cooperating owner of a Google Account, you will want to immediately serve the appropriate legal process to Google to preserve and obtain all available data associated with the Google Account. Detailed information about legal process for user data requests is publicly available as an FAQ here: https://support.google.com/transparencyreport/answer/7381738?hl=en

Examples of the kinds of data that may be available for each Google product or service is listed in the FAQ under the heading "What kinds of data do you disclose for different products?"

If and when legal authority allows, law enforcement and/or government officials should immediately submit a preservation request to Google LLC, followed by a Search Warrant, to preserve and then obtain all account content. Remember that anyone having the username and password for the Google Account(s) in question can remotely destroy data in their Google Account(s) at any time.

Legal Process requests for account data is submitted through the Google Law Enforcement Request System (LERS). Law Enforcement can create an account and login here: https://lers.google.com/signup_v2/landing

Additional contact information and/or information about serving legal process to Google LLC may be available to law enforcement and/or government officials from the Department of Justice, Computer Crime & Intellectual Property Section (CCIPS) or Search.org. Questions can be sent directly to the Google Legal Investigations Support team via email uslawenforcement@google.com.

Chromebook Forensic Acquisition

First and foremost, performing an acquisition of a Chromebook/Chromebox device is NOT the same as a traditional forensic acquisition performed on a "traditional" laptop or computer. You CANNOT change the BIOS/UEFI boot order to boot to an external USB forensic boot disk. You CANNOT boot a Chromebook/Chromebox with Paladin or any other common bootable forensic live USB. Any attempt to pull the hard drive and image the internal Chromebook/Chromebox storage will simply result in encrypted data that you can't get into. None of your previous tools and/or methods will acquire a Chromebook/Chromebox.

Because you are dealing with a device that contains encrypted "user vaults", you MUST have the username and password to be able to unlock the encrypted data and capture unencrypted data from the Chromebook/Chromebox. The "Encrypted Partition Recovery" process explained in this document will allow you to build a custom Recovery USB for you specific Chromebook/Chromebox model and then startup the device in a special recovery mode. In this special recovery mode, you will be able to extract encrypted user and (in some cases) system data from the device in an unencrypted state, providing you correctly authenticate with the correct username and password for each user.

Preparing for Chromebook Forensic Acquisition

This section provides information needed to create various specialized USB disks for use in various data acquisition scenarios.

What you need:

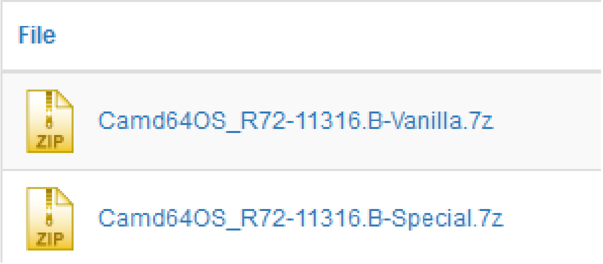
1. Three standard 32GB USB drives (do not use SD cards or other media). One to create a bootable live Chromium OS USB, one to create an Encrypted Partition Recovery USB drive used when you have the username and password for the account(s) on the Chromebook/Chromebox, and one to create a Physical Cloning Recovery USB drive that may only be used in very limited situations.

2. Provided custom bash scripts:
   1. create_encrypted_partition_recovery_usb.sh
   2. create_physical_cloning_recovery_usb.sh
   3. custom_chromeos-install
   4. image_chromebook.sh
   5. prep_evidence_drive.sh
   6. triage_stateful.sh
3. An additional USB drive of any kind, on which you will place the above provided bash scripts. Later you will mount the USB drive and copy the scripts from this USB to a /home/scripts/ folder on your Chromium OS live USB.
4. A large capacity portable USB3.0 hard drive large enough to hold a complete clone of the Chromebook/Chromebox internal HD you may be imaging. This will only be used in very limited situations and is not common. Preferably a very fast SSD drive with an external easily visible activity light, like the Samsung T5 shown below.

5. Chrome Browser, if not already installed and updated.
6. Chromebook Recovery Utility app, available here: https://chrome.google.com/webstore/detail/chromebook-recovery-

utili/jndclpdbaamdhonoechobihbbiimdgai

7. The “Special” build of Chromium for amd64 or x86 computers, Camd64OS_R72-11316.B-Special.7z for 64-bit computers, available here: https://chromium.arnoldthebat.co.uk/index.php?dir=special&order=modified&sort=desc



File

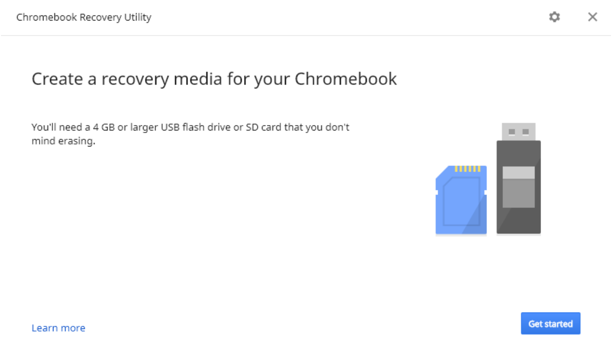
Camd64OS_R72-11316.B-Vanilla.7z

Camd64OS_R72-11316.B-Special.7z

8. If desired, you may manually download any of the past or present released builds of the ChromeOS Recovery USB image for your model Chromebook/Chromebox. These scripts and procedures were designed on release 72 and in the event future ChromeOS releases break these scripts or processes, you may need to go to this URL and use a build 72 or earlier Recovery image instead of the newer one produced by the Recovery Utility app. All builds are here: https://cros-updates-serving.appspot.com/

Create a factory ChromeOS Recovery USB drive

1. You must create unique Recovery USB drives for each model Chromebook/Chromebox device you wish to acquire. Each Recovery USB is designed for a specific model and will only work with that model. You will need to repeat these steps each time you need to acquire a new Chromebook/Chromebox device, using freshly created Recovery USB drives.
2. Your first step is to create factory ChromeOS Recovery USB drives for the specific Chromebook/Chromebook you need to acquire.
3. Run your Chrome Browser, type chrome://apps/ into the Chrome address bar, launch the Chromebook Recovery Utility app and click “Get Started.”

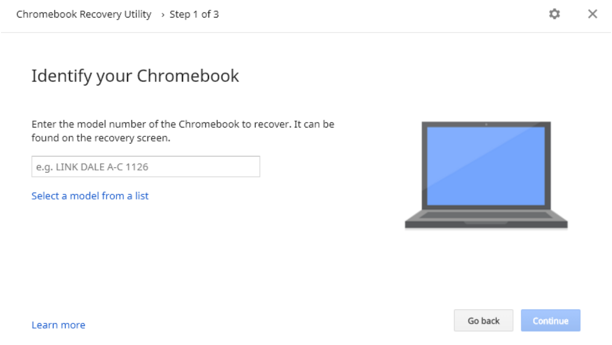


Chromebook Recovery Utility

Create a recovery media for your Chromebook

You'll need a 4 GB or larger USB flash drive or SD card that you don't mind erasing.

4. Click “Select a model from a list” and select your manufacturer and model from the dropdown boxes…



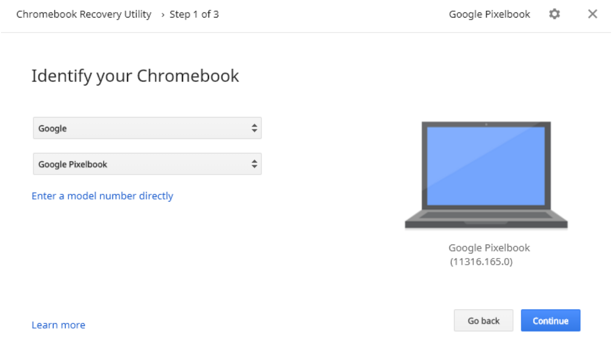
Chromebook Recovery Utility › Step 1 of 3

Identify your Chromebook

Enter the model number of the Chromebook to recover. It can be found on the recovery screen.

e.g. LINK DALE A-C 1126

…or enter a model # directly and click “Continue.”



Chromebook Recovery Utility › Step 1 of 3 Google Pixelbook

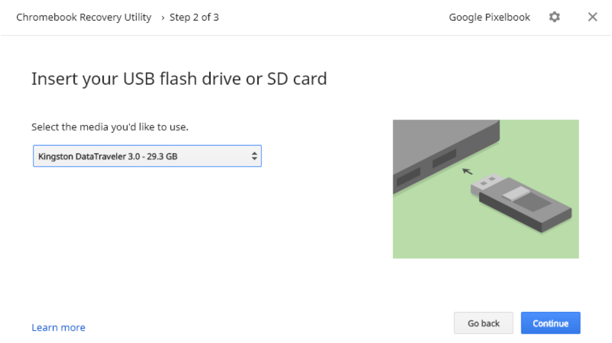
Identify your Chromebook

Google

Google Pixelbook

Google Pixelbook (11316.165.0)

5. Select your 32GB USB drive, on which you will be deploying one of the customized ChromeOS Recovery images discussed in this document, and click “Continue.”



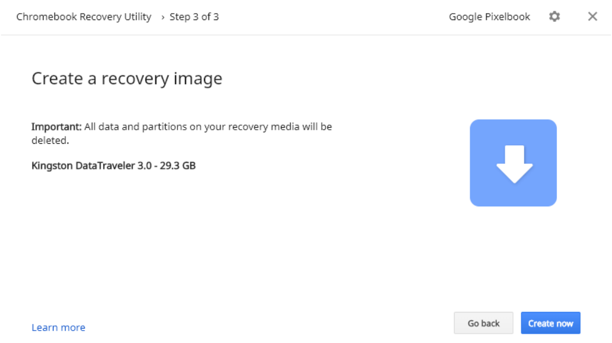
Chromebook Recovery Utility › Step 2 of 3 Google Pixelbook

Insert your USB flash drive or SD card

Select the media you'd like to use.

Kingston DataTraveler 3.0 - 29.3 GB

6. Click “Create now” to create a factory ChromeOS Recovery USB drive.



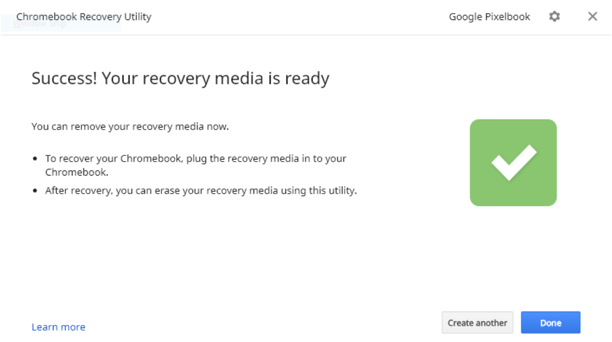
Chromebook Recovery Utility › Step 3 of 3 Google Pixelbook

Create a recovery image

Important: All data and partitions on your recovery media will be deleted.

Kingston DataTraveler 3.0 - 29.3 GB

7. When complete, safely eject your USB.
8. Click “Create another” to repeat the steps in this section to create a second factory ChromeOS Recovery USB drive, one to modify as an Encrypted Partition Recovery USB and one to modify as a Physical Cloning Recovery USB.



Chromebook Recovery Utility Google Pixelbook

Success! Your recovery media is ready

You can remove your recovery media now.

- To recover your Chromebook, plug the recovery media in to your Chromebook.
- After recovery, you can erase your recovery media using this utility.

9. Note that if you are performing these steps on a Windows OS, upon the creation of these ChromeOS USB drives, Windows will pop up NUMEROUS annoying dialog boxes asking if you want to format all of the many newly created partitions on the disk. Do NOT format or do anything other than simply close each and every pop-up dialog that appears.

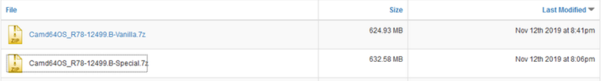
Create a Chromium OS live USB

1. The Chromium OS Live USB created in this section is designed to be used as a “utility” OS environment, in which you will be running various scripts to create your needed Recovery USBs or perform various functions. These “Special” build Chromium OS Live USBs need to be able to boot one of your forensic computers successfully so you can operate inside this Chromium OS environment. All of these procedures were successfully accomplished with Special builds 72 and 78, booting a MacBook Pro laptop. Testing with build 76 resulted in unsuccessful booting of that same MacBook Pro laptop due to video driver issues. Through trial and error, you may need to find the build (up through build 78 at the time of this release) that properly boots your forensic computer that you will be using. This step, and which Special build of Chromium that you use, will depend solely on the computer you will be booting with your Chromium OS Live USB.

   Note: Once you find a build that successfully boots your forensic computer, this Chromium OS Live USB does not need to be recreated each time you need to acquire a new Chromebook/Chromebox device and may be reused on your forensic computer for any subsequent creating of custom Recovery USB drives in the following sections of this document.

   Additionally, the build/version of Chromium OS that you use as this “utility” OS is insignificant and has NO bearing on the success or failure of performing the actual Encrypted Partition Recovery. You simply need ANY Chromium OS build to boot ANY of your personal computers to use as a platform to run ChromeOS bash scripts and interact with the filesystems on the special Chromebook recovery USBs.

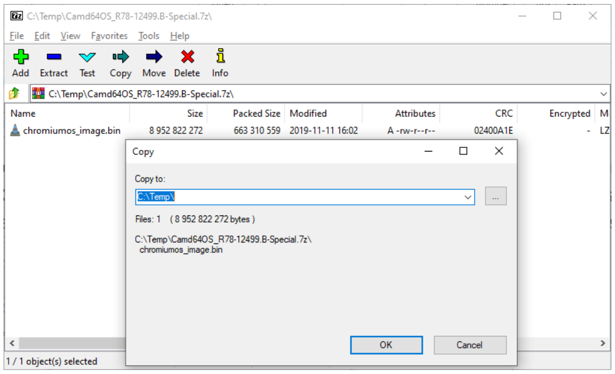
2. Download the “Special” build of Chromium for amd64 or x86 computers, Camd64OS_R78-12499.B-Special.7z for 64-bit computers, available here: https://chromium.arnoldthebat.co.uk/index.php?dir=special&order=modified&sort=desc

File	Size	Last Modified
Camd64OS_R78-12499.B-Vanilla.7z	624.93 MB	Nov 12th 2019 at 8:41pm
Camd64OS_R78-12499.B-Special.7z	632.58 MB	Nov 12th 2019 at 8:06pm

   Again, whichever “Special” build successfully boots your personal computer that you will use to build these custom Recovery USBs is adequate. No specific build is required.

3. Use 7-Zip to extract the image out of the 7z archive. Note, older releases called the image chromium_image.img but more recent releases of these Chromium images have been named chromium_image.bin instead. Regardless of what the name of the image is, simply extract the image contained in the 7-zip archive.



C:\Temp\Camd64OS_R78-12499.B-Special.7z\

C:\Temp\Camd64OS_R78-12499.B-Special.7z\

Name	Size	Packed Size	Modified	Attributes	CRC	Encrypted	M
chromiumos_image.bin	8 952 822 272	663 310 559	2019-11-11 16:02	A -rw-r--r--	02400A1E	-	LZ

1 / 1 object(s) selected

Copy

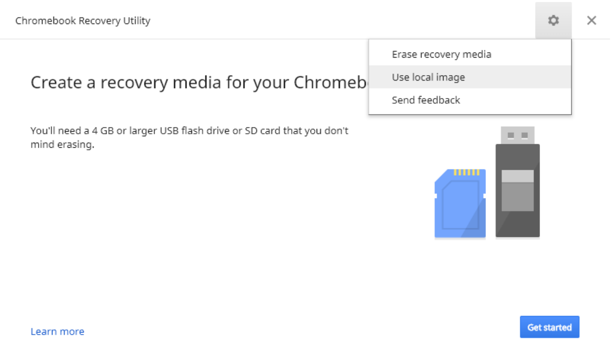
Copy to:

C:\Temp\

Files: 1 (8 952 822 272 bytes)

C:\Temp\Camd64OS_R78-12499.B-Special.7z\
chromiumos_image.bin

4. Launch the Chromebook Recovery Utility app and click the gear icon in the upper-right corner of the Chromebook Recovery Utility app.
chrome://apps/

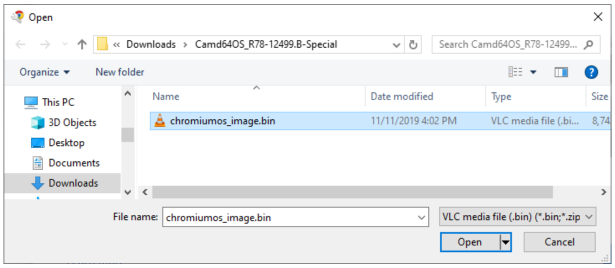


Chromebook Recovery Utility

Create a recovery media for your Chromeb

You'll need a 4 GB or larger USB flash drive or SD card that you don't mind erasing.

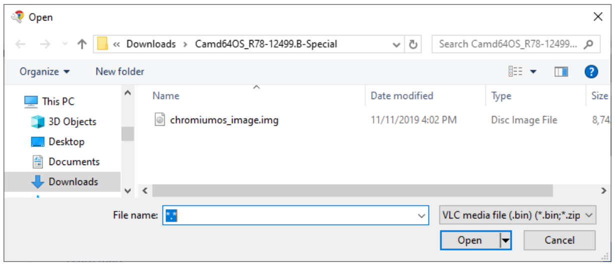
5. If your extracted Chromium OS image has a .bin file extension then the image file will be immediately visible when you browse to the folder containing the image. If your extracted Chromium OS image has an .img file extension, you will not immediately see the image file in the browse window where you select the downloaded and extracted “local image” and you must type “*.*” or “*.img” in the **File name:** box (as shown in the 2nd screenshot below, do NOT type *.* in the “search” box) to see and select the chromium_image.img image.



chromiumos_image.bin 11/11/2019 4:02 PM VLC media file (.bi... 8,74

File name: chromiumos_image.bin

VLC media file (.bin) (*.bin;*.zip

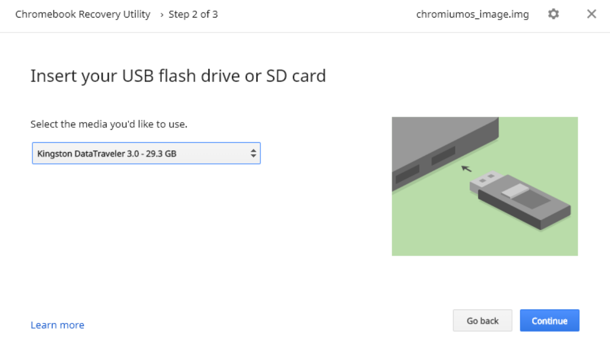


chromiumos_image.img 11/11/2019 4:02 PM Disc Image File 8,74

File name:

VLC media file (.bin) (*.bin;*.zip

6. Select a 32GB USB drive, on which you will be deploying the Chromium OS live USB image, and click “Continue.”

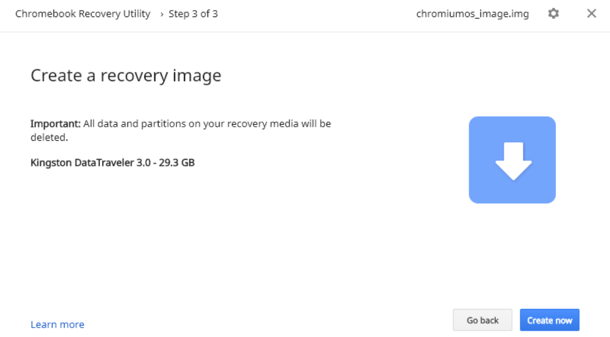


Insert your USB flash drive or SD card

Select the media you'd like to use.

Kingston DataTraveler 3.0 - 29.3 GB

7. Click “Create now” to create your Chromium OS live USB drive.



Create a recovery image

Important: All data and partitions on your recovery media will be deleted.

Kingston DataTraveler 3.0 - 29.3 GB

8. When complete, safely eject your USB and label the USB as your Chromium OS live USB.

9. Note that upon the creation of this USB drive, Windows will pop up NUMEROUS annoying dialog boxes asking if you want to format all of the many newly created partitions on the disk. Do NOT format or do anything other than simply close each and every pop-up dialog that appears.
10. If this Chromium OS live USB does not correctly boot your own forensic computer then you will need to repeat this section to find a “Special” build that does correctly boot your own computer, or try another forensic computer.

Copy provided scripts to your Chromium OS live USB

*Note: this section of the instructions requires at least some minimal understanding of *nix command line usage and commands.*

1. On your additional regular USB thumb drive, use Windows to create a folder in the root of the thumb drive called “scripts” and copy all provided bash scripts into that “scripts” folder.
2. Boot your own forensic computer to your newly created Chromium OS live USB.
3. Upon booting to Chromium OS, at the GUI splash screen, press CTRL+ALT+F2 to open a non-GUI pseudoterminal (TTY1 = /dev/pts/1), otherwise known as a terminal or console.
4. Log into TTY1 using “root” as the username and no password is required.
5. Plug in your USB thumb drive containing all the provided bash scripts in a “scripts” folder. The USB drive should contain ONLY the provided scripts in a “scripts” folder and nothing else!
6. At the terminal prompt, run “fdisk -l” so you can identify your USB drive containing the bash scripts.

7. At the terminal prompt, type “mktemp -d” and hit enter. Make note of the temporary folder created, as you will use this folder as a mount point to mount your USB drive containing the bash scripts. (i.e. temp folder created named /tmp/tmp.i4F2gtKrs)
8. Mount the partition of your USB drive that contains the bash scripts using the command “mount /dev/sdc1 /tmp/tmp.i4F2gtKrs5” where /dev/sdc1 must be the correct device and partition identifier for your USB drive containing the bash scripts. The /tmp/tmp.i4F2gtKrs5 part of the command must match the randomly generated folder created by the “mktemp -d” command.
9. Copy all files from /tmp/tmp.i4F2gtKrs5/scripts/ to a /home/scripts/ folder on your Chromium OS live USB using the command:
   mkdir /home/scripts && cp /tmp/tmp.i4F2gtKrs5/scripts/* /home/scripts/
10. Unmount the USB drive containing the bash scripts, using the command “umount /tmp/tmp.i4F2gtKrs5”
11. **Unplug the USB drive containing the bash scripts so it is no longer attached to the computer before running any of the scripts!**

Create your Encrypted Partition Recovery USB drive

1. Attach one of your previously created factory ChromeOS Recovery USB drive to your forensic computer, which you have currently booted to Chromium OS using your Chromium OS live USB.
2. Run the bash script to turn the factory ChromeOS Recovery USB drive into an Encrypted Partition Recovery USB drive, using the command:
   “. /home/scripts/create_encrypted_partition_recovery_usb.sh” without the quotes. Make sure you have a space between the ‘.’ and /home/scripts/create_encrypted_partition_recovery_usb.sh.
3. You will be prompted to select the attached factory ChromeOS Recovery USB and then have the opportunity to choose the partition size to be created on the USB. The default partition size is 10GB and you can take the default unless you know you need a larger partition for capture of a very large amount of encrypted user data.
4. Read each prompt and/or information provided by the script. Confirm “Y” at each prompt in the script until the script ends.
5. The factory ChromeOS Recovery USB is now an Encrypted Partition Recovery USB to be used solely for the purpose of acquiring a decrypted logical backup of encrypted data on a Chromebook/Chromebox device for which you have a username and password.
6. Remove the USB drive and label the USB as your Encrypted Partition Recovery USB.

7. Do not shutdown Chromium OS yet. Continue with the next section.

Create your Physical Cloning Recovery USB drive

Note: this Physical Cloning Recovery USB and Clone Destination output USB are NOT used in most situations. A Physical Clone of a Chromebook/Chromebox will result in a “dd” image containing encrypted data. At the time of this writing, there are no publicly available tools and/or methods to decrypt an encrypted image from a Chromebook/Chromebox. Therefore, unless you are taking a clone image for future preservation, with the hopes that you can someday decrypt it, taking a physical clone will result in unusable data being captured.

If your Chromebook/Chromebox is already in “Developer Mode” (discussed further later in this paper), and you wish to proceed and perform a physical clone acquisition, the following steps will help you create the needed custom recovery USB.

1. Attach your second previously created factory ChromeOS Recovery USB drive to your forensic computer, which you have currently booted to Chromium OS using your Chromium OS live USB.
2. Run the bash script to turn the factory ChromeOS Recovery USB drive into a Physical Cloning Recovery USB, using the command: “. /home/scripts/create_physical_cloning_recovery_usb.sh” without the quotes. Make sure you have a space between the ‘.’ and /home/scripts/create_physical_cloning_recovery_usb.sh.
3. The factory ChromeOS Recovery USB is now a Physical Cloning Recovery USB to be used solely for the purpose of capturing a full physical clone of the hard drive of a seized Chromebook/Chromebox device.
4. Remove the USB drive and label the USB as your Physical Cloning Recovery USB.

5. Do not shutdown Chromium OS yet. Continue with the next section.

Prepare your clone destination output USB hard drive

1. You may, if desired and in certain circumstances, be cloning the internal HD of a seized Chromebook/Chromebox to your large capacity USB3.0 hard drive. You MUST first completely WIPE your large capacity USB hard drive using whatever method you choose before completing any further preparation steps, to ensure the destination drive contains no residual data.
2. After the destination USB drive is wiped, attach it to your forensic computer running Chromium OS from the previous section of this document.
3. Run the bash script to prepare the wiped destination USB drive so that it is ready to be cloned with the internal HD of your seized Chromebook/Chromebox. Use the command:
   “. /home/scripts/prep_evidence_drive.sh” without the quotes. Make sure you have a space between the ‘.’ and /home/scripts/prep_evidence_drive.sh.
4. When prompted by the script, select the number identified as your wiped destination USB drive.
5. You will be prompted to confirm that you wish to re-write new partitioning information to the selected disk. Hit “Y” or “y” to confirm and finish preparing the destination USB drive.
6. You may now disconnect your prepared destination USB drive, label the USB as your Evidence Destination USB, and shutdown Chromium OS.

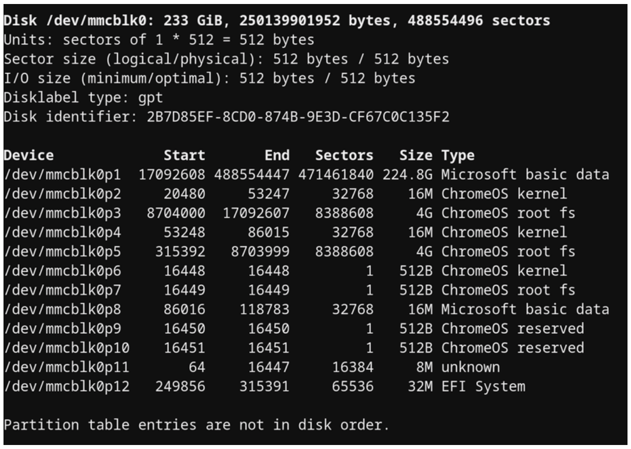
Logical Encrypted Partition Recovery

This section of the document is for use when you either 1) have a cooperating individual that provides you with the username and password for the user account(s) setup on a Chromebook/Chromebox; or 2) you obtain the username(s) and password(s) from other means.

Note that any Chromebook/Chromebox can be in either “Normal mode” or “Developer Mode” when using this process. Either way, this process recovers decrypted data from the users’ encrypted vault and/or encrypted.block system file on the “STATE” partition (i.e. stateful_partition) of the Chromebook/Chromebox device and leaves the device in its pre-existing operational status.

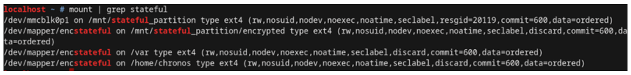
What exactly do you hope to recover/acquire?

Chromebook/Chromebox devices have a complex hard drive partitioning scheme. There are several small partitions that contain non-user data including copies of the ChromeOS kernel, root file systems, and EFI firmware. Partition 1 (/dev/mmcblk0p1 shown below) is the largest partition on the hard drive and contains user and system data of evidentiary value. The screenshot below demonstrates the default partitioning scheme on the 256GB drive of a Google Pixelbook.



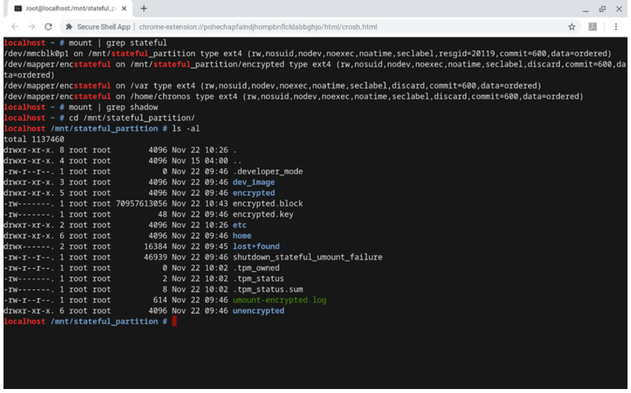
```
Disk /dev/mmcblk0: 233 GiB, 250139901952 bytes, 488554496 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 2B7D85EF-8CD0-874B-9E3D-CF67C0C135F2

Device             Start       End   Sectors   Size Type
/dev/mmcblk0p1  17092608 488554447 471461840 224.8G Microsoft basic data
/dev/mmcblk0p2     20480     53247     32768    16M ChromeOS kernel
/dev/mmcblk0p3   8704000  17092607   8388608     4G ChromeOS root fs
/dev/mmcblk0p4     53248     86015     32768    16M ChromeOS kernel
/dev/mmcblk0p5    315392   8703999   8388608     4G ChromeOS root fs
/dev/mmcblk0p6     16448     16448         1   512B ChromeOS kernel
/dev/mmcblk0p7     16449     16449         1   512B ChromeOS root fs
/dev/mmcblk0p8     86016    118783     32768    16M Microsoft basic data
/dev/mmcblk0p9     16450     16450         1   512B ChromeOS reserved
/dev/mmcblk0p10    16451     16451         1   512B ChromeOS reserved
/dev/mmcblk0p11       64     16447     16384     8M unknown
/dev/mmcblk0p12   249856    315391     65536    32M EFI System

Partition table entries are not in disk order.
```

Partition 1 has a volume label called “STATE”, and it is known as and mounted by ChromeOS as the “Stateful Partition”. ChromeOS mounts this partition to the folder mountpoint /mnt/stateful_partition as shown in the below screenshot.



```
localhost ~ # mount | grep stateful
/dev/mmcblk0p1 on /mnt/stateful_partition type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,resgid=20119,commit=600,data=ordered)
/dev/mapper/encstateful on /mnt/stateful_partition/encrypted type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,discard,commit=600,da
ta=ordered)
/dev/mapper/encstateful on /var type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,discard,commit=600,data=ordered)
/dev/mapper/encstateful on /home/chronos type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,discard,commit=600,data=ordered)
```

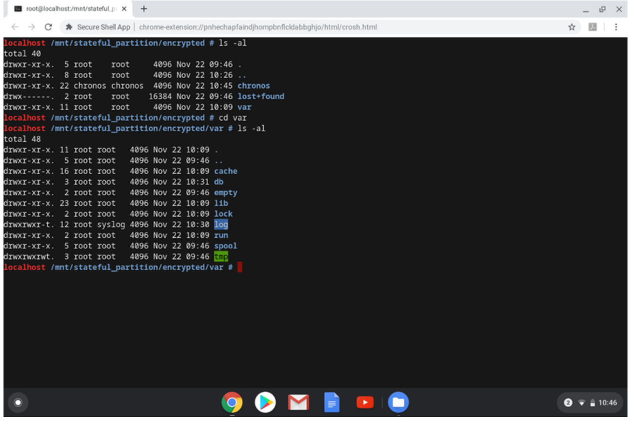
Contained in the root of the STATE partition, is an encrypted block of volatile data in a file called encrypted.block. Upon successful boot of ChromeOS, this encrypted.block is decrypted into the mountpoint folders /mnt/stateful_partition/encrypted, /var, and /home/chronos. These mountpoint folders contain all kinds of user-attributable system data of evidentiary value.



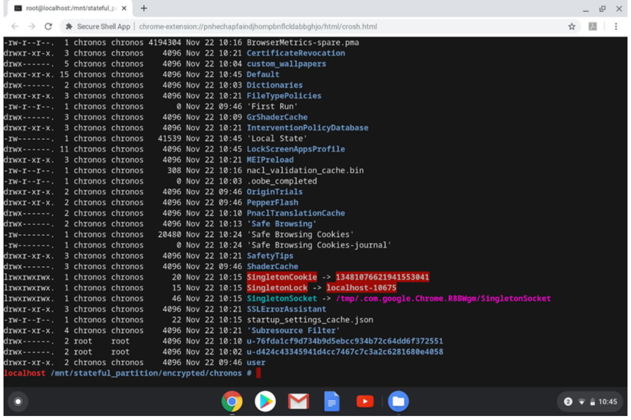
root@localhost:/mnt/stateful_p
Secure Shell App
chrome-extension://pnhechapfaindjhompbnflcldabbghjo/html/crosh.html

```
localhost ~ # mount | grep stateful
/dev/mmcblk0p1 on /mnt/stateful_partition type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,resgid=20119,commit=600,data=ordered)
/dev/mapper/encstateful on /mnt/stateful_partition/encrypted type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,discard,commit=600,da
ta=ordered)
/dev/mapper/encstateful on /var type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,discard,commit=600,data=ordered)
/dev/mapper/encstateful on /home/chronos type ext4 (rw,nosuid,nodev,noexec,noatime,seclabel,discard,commit=600,data=ordered)
localhost ~ # mount | grep shadow
localhost ~ # cd /mnt/stateful_partition/
localhost /mnt/stateful_partition # ls -al
total 1137460
drwxr-xr-x. 8 root root        4096 Nov 22 10:26 .
drwxr-xr-x. 4 root root        4096 Nov 15 04:00 ..
-rw-r--r--. 1 root root           0 Nov 22 09:46 .developer_mode
drwxr-xr-x. 3 root root        4096 Nov 22 09:46 dev_image
drwxr-xr-x. 5 root root        4096 Nov 22 09:46 encrypted
-rw-------. 1 root root 70957613056 Nov 22 10:43 encrypted.block
-rw-------. 1 root root          48 Nov 22 09:46 encrypted.key
drwxr-xr-x. 2 root root        4096 Nov 22 10:26 etc
drwxr-xr-x. 6 root root        4096 Nov 22 09:46 home
drwx------. 2 root root       16384 Nov 22 09:45 lost+found
-rw-r--r--. 1 root root       46939 Nov 22 09:46 shutdown_stateful_umount_failure
-rw-r--r--. 1 root root           0 Nov 22 10:02 .tpm_owned
-rw-------. 1 root root           2 Nov 22 10:02 .tpm_status
-rw-------. 1 root root           8 Nov 22 10:02 .tpm_status.sum
-rw-r--r--. 1 root root         614 Nov 22 09:46 umount-encrypted.log
drwxr-xr-x. 6 root root        4096 Nov 22 09:46 unencrypted
localhost /mnt/stateful_partition #
```

Here are some examples of the contents of the decrypted “encrypted.block” file.



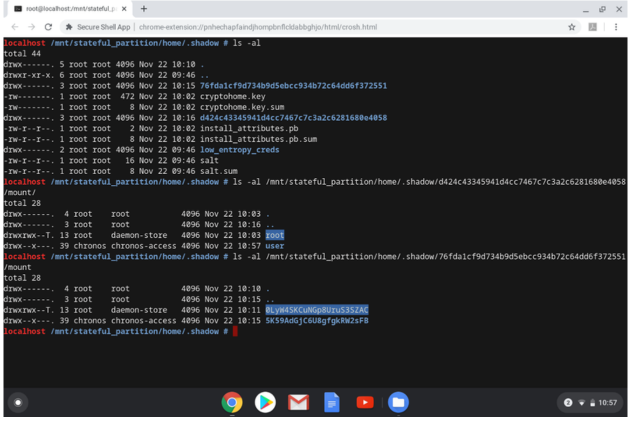
```
localhost /mnt/stateful_partition/encrypted # ls -al
total 40
drwxr-xr-x.  5 root    root     4096 Nov 22 09:46 .
drwxr-xr-x.  8 root    root     4096 Nov 22 10:26 ..
drwxr-xr-x. 22 chronos chronos  4096 Nov 22 10:45 chronos
drwx------.  2 root    root    16384 Nov 22 09:46 lost+found
drwxr-xr-x. 11 root    root     4096 Nov 22 10:09 var
localhost /mnt/stateful_partition/encrypted # cd var
localhost /mnt/stateful_partition/encrypted/var # ls -al
total 48
drwxr-xr-x. 11 root root   4096 Nov 22 10:09 .
drwxr-xr-x.  5 root root   4096 Nov 22 09:46 ..
drwxr-xr-x. 16 root root   4096 Nov 22 10:09 cache
drwxr-xr-x.  3 root root   4096 Nov 22 10:31 db
drwxr-xr-x.  2 root root   4096 Nov 22 09:46 empty
drwxr-xr-x. 23 root root   4096 Nov 22 10:09 lib
drwxr-xr-x.  2 root root   4096 Nov 22 10:09 lock
drwxrwxr-t. 12 root syslog 4096 Nov 22 10:30 log
drwxr-xr-x.  2 root root   4096 Nov 22 10:09 run
drwxr-xr-x.  5 root root   4096 Nov 22 09:46 spool
drwxrwxrwt.  3 root root   4096 Nov 22 09:46 tmp
localhost /mnt/stateful_partition/encrypted/var #
```



```
-rw-r--r--.  1 chronos chronos 4194304 Nov 22 10:16 BrowserMetrics-spare.pma
drwxr-xr-x.  3 chronos chronos    4096 Nov 22 10:21 CertificateRevocation
drwx------.  5 chronos chronos    4096 Nov 22 10:04 custom_wallpapers
drwxr-xr-x. 15 chronos chronos    4096 Nov 22 10:45 Default
drwx------.  2 chronos chronos    4096 Nov 22 10:03 Dictionaries
drwxr-xr-x.  3 chronos chronos    4096 Nov 22 10:21 FileTypePolicies
-rw-r--r--.  1 chronos chronos       0 Nov 22 09:46 'First Run'
drwx------.  3 chronos chronos    4096 Nov 22 10:09 GrShaderCache
drwxr-xr-x.  3 chronos chronos    4096 Nov 22 10:21 InterventionPolicyDatabase
-rw-------.  1 chronos chronos   41539 Nov 22 10:45 'Local State'
drwx------. 11 chronos chronos    4096 Nov 22 10:45 LockScreenAppsProfile
drwxr-xr-x.  3 chronos chronos    4096 Nov 22 10:21 MEIPreload
-rw-r--r--.  1 chronos chronos     308 Nov 22 10:16 nacl_validation_cache.bin
-rw-r--r--.  1 chronos chronos       0 Nov 22 10:03 .oobe_completed
drwxr-xr-x.  2 chronos chronos    4096 Nov 22 09:46 OriginTrials
drwxr-xr-x.  2 chronos chronos    4096 Nov 22 09:46 PepperFlash
drwx------.  2 chronos chronos    4096 Nov 22 10:10 PnaclTranslationCache
drwx------.  2 chronos chronos    4096 Nov 22 10:13 'Safe Browsing'
-rw-------.  1 chronos chronos   20480 Nov 22 10:24 'Safe Browsing Cookies'
-rw-------.  1 chronos chronos       0 Nov 22 10:24 'Safe Browsing Cookies-journal'
drwxr-xr-x.  3 chronos chronos    4096 Nov 22 10:21 SafetyTips
drwx------.  3 chronos chronos    4096 Nov 22 09:46 ShaderCache
lrwxrwxrwx.  1 chronos chronos      20 Nov 22 10:15 SingletonCookie -> 13481076621941553041
lrwxrwxrwx.  1 chronos chronos      15 Nov 22 10:15 SingletonLock -> localhost-10675
lrwxrwxrwx.  1 chronos chronos      46 Nov 22 10:15 SingletonSocket -> /tmp/.com.google.Chrome.R8BWgm/SingletonSocket
drwxr-xr-x.  3 chronos chronos    4096 Nov 22 10:21 SSLErrorAssistant
-rw-r--r--.  1 chronos chronos      22 Nov 22 10:15 startup_settings_cache.json
drwxr-xr-x.  4 chronos chronos    4096 Nov 22 10:21 'Subresource Filter'
drwx------.  2 root    root       4096 Nov 22 10:10 u-76fda1cf9d734b9d5ebcc934b72c64dd6f372551
drwx------.  2 root    root       4096 Nov 22 10:02 u-d424c43345941d4cc7467c7c3a2c6281680e4058
drwxr-xr-x.  2 chronos chronos    4096 Nov 22 09:46 user
localhost /mnt/stateful_partition/encrypted/chronos #
```

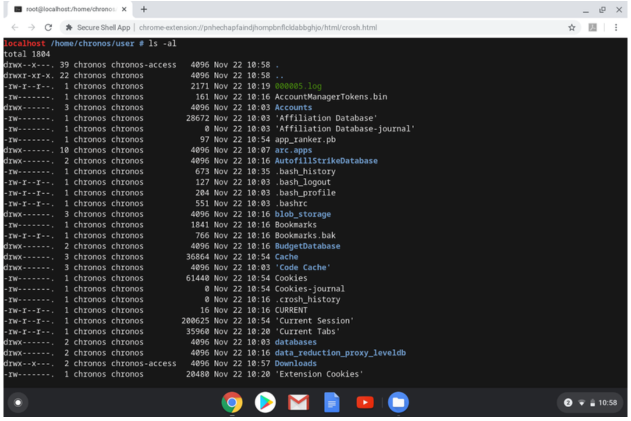
Additionally, each user on the Chromebook/Chromebox has their own user-specific encrypted vault where all their user data is stored. These encrypted vaults are only accessible in a decrypted form when the user logs in with the correct username and password. The encrypted vaults consist of a series of folders, subfolders and files contained within the /mnt/stateful_partition/home/.shadow folder of the mounted "STATE" partition.

The below screenshot shows that this Pixelbook currently has two user accounts, and therefore two encrypted user vaults, contained in folders called 76fda1cf9d734b9d5ebcc934b72c64dd6f372551 and d424c43345941d4cc7467c7c3a2c6281680e4058. The vault starting with d424… is currently logged on and decrypted and the vault starting with 76dfa… is not logged on and is therefore is still encrypted.


root@localhost:/mnt/stateful_p
Secure Shell App | chrome-extension://pnhechapfaindjhompbnflcldabbghjo/html/crosh.html
10:57

```
localhost /mnt/stateful_partition/home/.shadow # ls -al
total 44
drwx------. 5 root root 4096 Nov 22 10:10 .
drwxr-xr-x. 6 root root 4096 Nov 22 09:46 ..
drwx------. 3 root root 4096 Nov 22 10:15 76fda1cf9d734b9d5ebcc934b72c64dd6f372551
-rw-------. 1 root root  472 Nov 22 10:02 cryptohome.key
-rw-------. 1 root root    8 Nov 22 10:02 cryptohome.key.sum
drwx------. 3 root root 4096 Nov 22 10:16 d424c43345941d4cc7467c7c3a2c6281680e4058
-rw-r--r--. 1 root root    2 Nov 22 10:02 install_attributes.pb
-rw-r--r--. 1 root root    8 Nov 22 10:02 install_attributes.pb.sum
drwx------. 2 root root 4096 Nov 22 09:46 low_entropy_creds
-rw-r--r--. 1 root root   16 Nov 22 09:46 salt
-rw-r--r--. 1 root root    8 Nov 22 09:46 salt.sum
localhost /mnt/stateful_partition/home/.shadow # ls -al /mnt/stateful_partition/home/.shadow/d424c43345941d4cc7467c7c3a2c6281680e4058
/mount/
total 28
drwx------.  4 root    root           4096 Nov 22 10:03 .
drwx------.  3 root    root           4096 Nov 22 10:16 ..
drwxrwx--T. 13 root    daemon-store   4096 Nov 22 10:03 root
drwx--x---. 39 chronos chronos-access 4096 Nov 22 10:57 user
localhost /mnt/stateful_partition/home/.shadow # ls -al /mnt/stateful_partition/home/.shadow/76fda1cf9d734b9d5ebcc934b72c64dd6f372551
/mount
total 28
drwx------.  4 root    root           4096 Nov 22 10:10 .
drwx------.  3 root    root           4096 Nov 22 10:15 ..
drwxrwx--T. 13 root    daemon-store   4096 Nov 22 10:11 0LyW4SKCuNGp8UruS3SZAC
drwx--x---. 39 chronos chronos-access 4096 Nov 22 10:15 5K59AdGjC6U8gfgkRW2sFB
localhost /mnt/stateful_partition/home/.shadow #
```

Your Encrypted Partition Recovery USB will perform a decrypted extraction of the contents of the encrypted user vault of your choice, providing you have the correct username and password. An example of the data to be decrypted and extracted is shown below, including the contents of the user's Downloads folder and all other user-attributable data for this user.


root@localhost:/home/chronos/
Secure Shell App | chrome-extension://pnhechapfaindjhompbnflcldabbghjo/html/crosh.html
10:58

```
localhost /home/chronos/user # ls -al
total 1804
drwx--x---. 39 chronos chronos-access   4096 Nov 22 10:58 .
drwxr-xr-x. 22 chronos chronos          4096 Nov 22 10:58 ..
-rw-r--r--.  1 chronos chronos          2171 Nov 22 10:19 000005.log
-rw-------.  1 chronos chronos           161 Nov 22 10:16 AccountManagerTokens.bin
drwx------.  3 chronos chronos          4096 Nov 22 10:03 Accounts
-rw-------.  1 chronos chronos         28672 Nov 22 10:03 'Affiliation Database'
-rw-------.  1 chronos chronos             0 Nov 22 10:03 'Affiliation Database-journal'
-rw-------.  1 chronos chronos            97 Nov 22 10:54 app_ranker.pb
drwx------. 10 chronos chronos          4096 Nov 22 10:07 arc.apps
drwx------.  2 chronos chronos          4096 Nov 22 10:16 AutofillStrikeDatabase
-rw-------.  1 chronos chronos           673 Nov 22 10:35 .bash_history
-rw-r--r--.  1 chronos chronos           127 Nov 22 10:03 .bash_logout
-rw-r--r--.  1 chronos chronos           204 Nov 22 10:03 .bash_profile
-rw-r--r--.  1 chronos chronos           551 Nov 22 10:03 .bashrc
drwx------.  3 chronos chronos          4096 Nov 22 10:16 blob_storage
-rw-------.  1 chronos chronos          1841 Nov 22 10:16 Bookmarks
-rw-r--r--.  1 chronos chronos           766 Nov 22 10:16 Bookmarks.bak
drwx------.  2 chronos chronos          4096 Nov 22 10:16 BudgetDatabase
drwx------.  3 chronos chronos         36864 Nov 22 10:54 Cache
drwx------.  3 chronos chronos          4096 Nov 22 10:03 'Code Cache'
-rw-------.  1 chronos chronos         61440 Nov 22 10:54 Cookies
-rw-------.  1 chronos chronos             0 Nov 22 10:54 Cookies-journal
-rw-------.  1 chronos chronos             0 Nov 22 10:16 .crosh_history
-rw-r--r--.  1 chronos chronos            16 Nov 22 10:16 CURRENT
-rw-r--r--.  1 chronos chronos        200625 Nov 22 10:54 'Current Session'
-rw-r--r--.  1 chronos chronos         35960 Nov 22 10:20 'Current Tabs'
drwx------.  2 chronos chronos          4096 Nov 22 10:03 databases
drwx------.  2 chronos chronos          4096 Nov 22 10:16 data_reduction_proxy_leveldb
drwx--x---.  2 chronos chronos-access   4096 Nov 22 10:57 Downloads
-rw-------.  1 chronos chronos         20480 Nov 22 10:20 'Extension Cookies'
```

If the user account is the "owner" account on the Chromebook/Chromebox then in addition to the decrypted user vault, you will also get the entire decrypted contents of the system data contained in the encrypted.block file. If the user account you extract is not the "owner" account on the device, then you will only be provided the decrypted user vault for that user without the extra system data.

On a Chromebook/Chromebox with only one user account, that user account is the "owner" account. On a Chromebook/Chromebox with multiple user accounts, the first account setup is the "owner" account. You can check for the "owner" account on the initial login screen of a booted Chromebook/Chromebox by clicking on the drop-down arrow to the right of any username on the login screen.

Phases of the Encrypted Partition Recovery process

The sequence of the Encrypted Partition Recovery Process is as follows:

1. Phase 1:

a. Shutdown the Chromebook/Chromebox and restart the device in “Recovery Mode”

b. Follow the onscreen instructions to insert a “Recovery USB” to perform a device recovery.

i. Normally, this is done to reset a Chromebook/Chromebox to its factory settings using a regular “factory recovery USB”. However, you are using a custom “Encrypted Partition Recovery USB” instead that starts a different process.

c. The device recognizes the special recovery USB and invokes the first phase of the Encrypted Partition Recovery after waiting 150 seconds.

d. The device will prompt you for the username and password of the account you wish to recover. Upon entering the username and password, the device will restart and continue the next process

e. Upon restart, the device will sit at the GUI login screen. While you are sitting at the GUI login screen, in the background the ChromeOS is creating a temporary copy of all encrypted data that will be recovered, storing the temporary unencrypted files on the internal storage of the Chromebook/Chromebox.

f. Once done creating the decrypted copy of all files (OR AFTER RUNNING OUT OF FREE DISK SPACE ON THE DEVICE), the device will conclude Phase 1 and restart to a recovery screen.

2. Phase 2:

a. Shutdown the device from the recovery screen at the end of Phase 1 and restart again into “Recovery Mode”

b. Follow the onscreen instructions to insert a “Recovery USB” and re-insert the same custom Encrypted Partition Recovery USB that you used in Phase 1.

c. The ChromeOS on the device will detect that a previous Encrypted Partition Recovery is in progress and will again wait 150 seconds.

d. The Encrypted Partition Recovery process will then start packaging all of the previously decrypted files created during Phase 1 into the final extracted.tgz archive on your USB.

i. This part may take a while, depending on the amount of data being compressed into the extracted.tgz, so be patient.

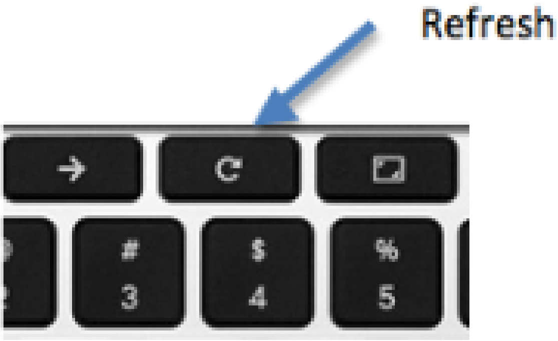
ii. If this goes really quickly, it is most likely that your username and password used for the recovery is either incorrect or was typed incorrectly.

e. When the creation of the extracted.tgz file is complete, the ChromeOS removes all of the previously created temporary copies of the decrypted files from the device's internal storage.

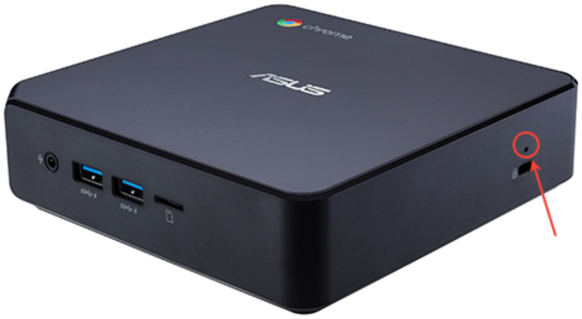
f. Once done, you shut down the device and remove your USB.

Performing the Encrypted Partition Recovery

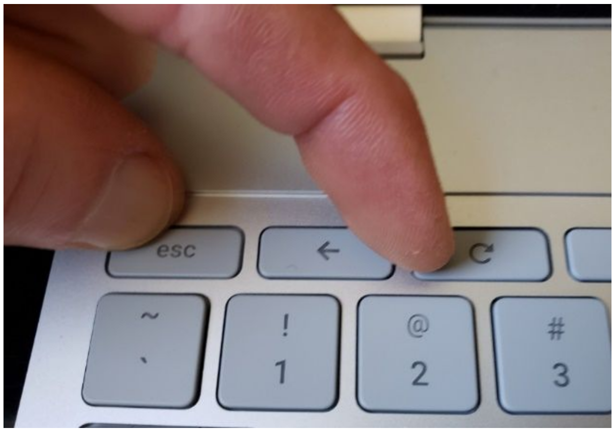
1. Read all steps in this section in their entirety before you go through this process! There are certain steps that MUST be followed EXACTLY as explained!
2. Phase 1:
   From a powered off Chromebook/Chromebox, place the device in "Recovery Mode". Certain model Chromebooks require holding a keyboard sequence "ESC+Refresh" while powering on the Chromebook. Other models, such as Chromeboxes, have a physical recovery button/switch that must be pressed/switched while powering on the Chromebook. See further information under the "Enter Recovery Mode" section of this support page from Google.
   https://support.google.com/chromebook/answer/1080595?hl=en



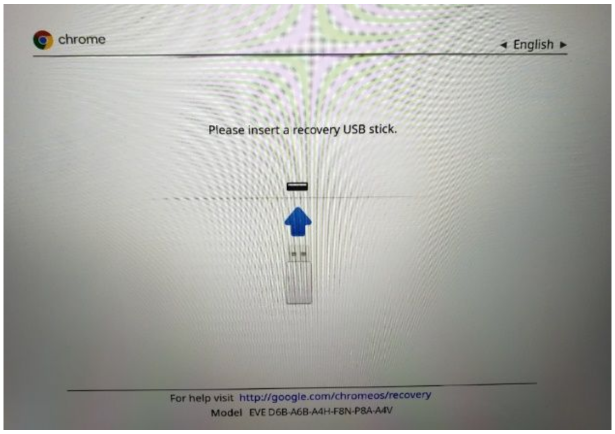
or



3. When powered on to Recovery Mode, you will see this on the screen saying “Please insert a recovery USB stick.”



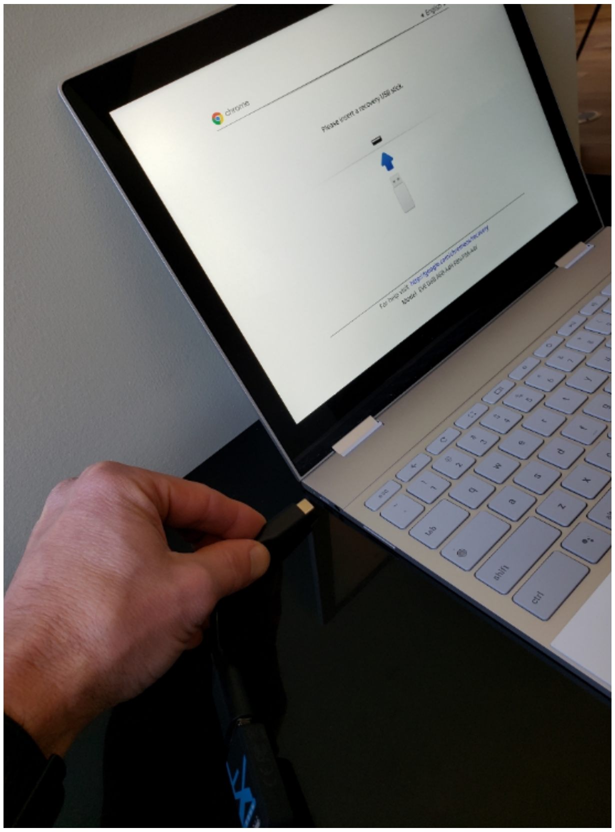
>



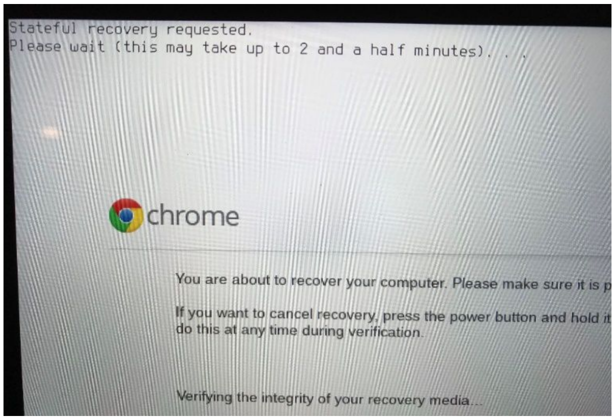
Please insert a recovery USB stick.

For help visit http://google.com/chromeos/recovery
Model EVE D6B-A6B-A4H-F8N-P8A-A4V

4. Insert your Encrypted Partition Recovery USB drive to automatically start the “Stateful Recovery” process.



5. After a few seconds, the screen will go blank and you will then see the below screens appear.



```
Stateful recovery requested.
Please wait (this may take up to 2 and a half minutes). . .
```

chrome

You are about to recover your computer. Please make sure it is p

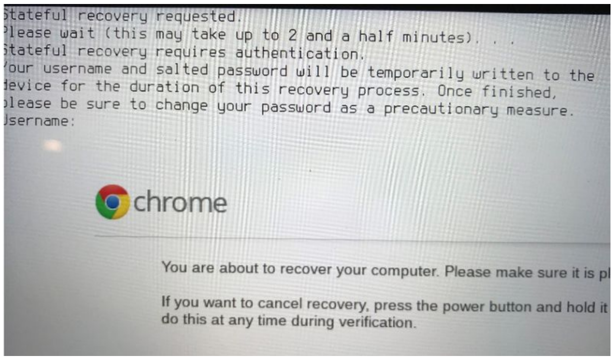
If you want to cancel recovery, press the power button and hold it
do this at any time during verification.

Verifying the integrity of your recovery media...

6. If you see anything other than the above screen stating “Stateful recovery requested”, you will have a short wait period during which you must immediately press and hold down the power button to force the Chromebook/Chromebox to power down before any data is destroyed.
7. You will be prompted to enter the username (email address) and password of the user account, of which you will capture a decrypted backup of the contents of the

user’s encrypted vault. If the user entered is the system “Owner” (i.e. the first Google Account setup on the computer, if there are multiple accounts setup.) then the decrypted backup will also include all system data contained in the encrypted.block file found in the root of the stateful partition. This system data contains a significant amount of data that may be of interest. If the user entered is NOT the system owner then only the user’s vault will be decrypted and backed up. This decrypted backup process may be repeated for each user you have the username/password for, one user at a time.

Note: Google does not use special characters in the prefix of email addresses, so you must type first.last@gmail.com as firstlast@gmail.com

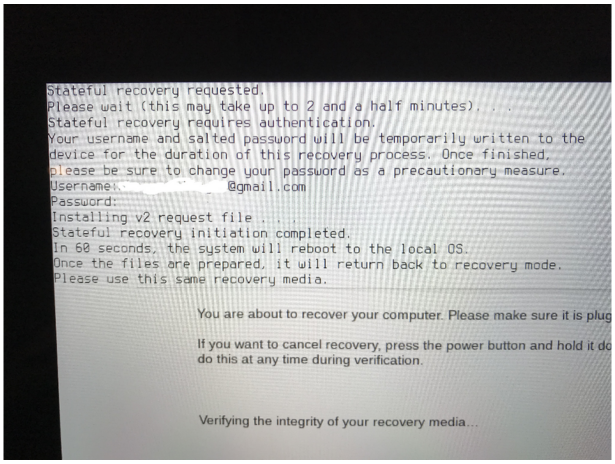


```
Stateful recovery requested.
Please wait (this may take up to 2 and a half minutes). . .
Stateful recovery requires authentication.
Your username and salted password will be temporarily written to the
device for the duration of this recovery process. Once finished,
please be sure to change your password as a precautionary measure.
Username:
```

You are about to recover your computer. Please make sure it is pl

If you want to cancel recovery, press the power button and hold it
do this at any time during verification.

8. After entering the username and password, just be patient while the system reboots.



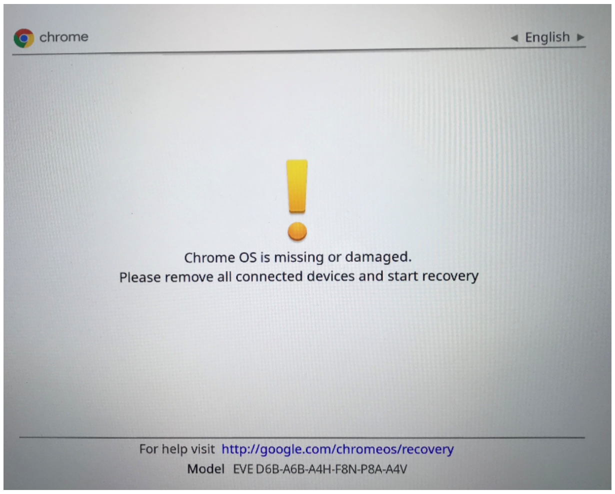
```
Stateful recovery requested.
Please wait (this may take up to 2 and a half minutes). . .
Stateful recovery requires authentication.
Your username and salted password will be temporarily written to the
device for the duration of this recovery process. Once finished,
please be sure to change your password as a precautionary measure.
Username:[redacted]@gmail.com
Password:
Installing v2 request file . . .
Stateful recovery initiation completed.
In 60 seconds, the system will reboot to the local OS.
Once the files are prepared, it will return back to recovery mode.
Please use this same recovery media.
```

You are about to recover your computer. Please make sure it is plug

If you want to cancel recovery, press the power button and hold it do
do this at any time during verification.

Verifying the integrity of your recovery media...

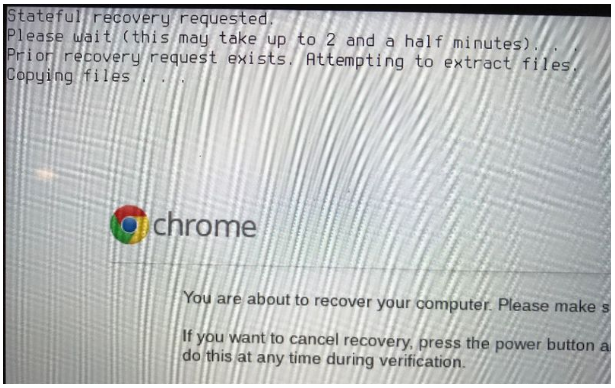
The system will now reboot to the normal ChromeOS login screen and perform some processes in the background. Do not attempt to login or do anything, just be patient and wait. On some systems after the login screen disappears and then attempts to restart to start the copy process, you see the below screen saying “ChromeOS is missing or damaged.” If this appears, this is normal (nothing is corrupt or missing) and you should continue with steps 10 and 11. On some systems, this “Chrome OS is missing or damaged” message does not appear and the process automatically restarts in Recovery Mode and automatically continues with step 12 below, skipping steps 10 and 11. If the below screen appears, continue with step 10. If the below screen does not appear, and the device restarts automatically into “Phase 2”, continue with step 11 below.



Chrome OS is missing or damaged.
Please remove all connected devices and start recovery

For help visit http://google.com/chromeos/recovery
Model EVE D6B-A6B-A4H-F8N-P8A-A4V

9. Disconnect your Encrypted Partition Recovery USB drive and power off the Chromebook/Chromebox.
10. Restart the Chromebook/Chromebox in Recovery Mode again and insert the same Encrypted Partition Recovery USB drive you just disconnected.
11. Phase 2:
    Be patient and wait until you see the message that the recovery process is copying files. Note: Having USB devices with activity lights makes it easier to watch and ensure that the copying is taking place.

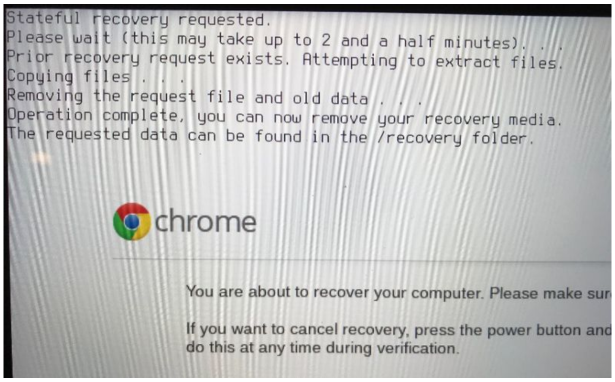


```
Stateful recovery requested.
Please wait (this may take up to 2 and a half minutes). . .
Prior recovery request exists. Attempting to extract files.
Copying files . . .
```

You are about to recover your computer. Please make s

If you want to cancel recovery, press the power button a
do this at any time during verification.

12. When the Copying Files process is complete you will be instructed to disconnect your USB and shutdown. Your USB now contains a file called extracted.tgz in a recovery folder created on the STATE partition (partition 1) of your Encrypted Partition Recovery USB drive.

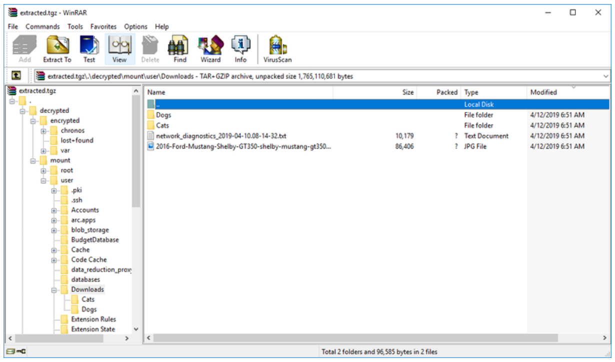


```
Stateful recovery requested.
Please wait (this may take up to 2 and a half minutes). . .
Prior recovery request exists. Attempting to extract files.
Copying files . . .
Removing the request file and old data . . .
Operation complete, you can now remove your recovery media.
The requested data can be found in the /recovery folder.
```

You are about to recover your computer. Please make sur

If you want to cancel recovery, press the power button and
do this at any time during verification.

13. This tar gzip archive contains the decrypted backup of your requested files. You may mount partition 1 of your Encrypted Partition Recovery USB drive using your Chromium live USB and extract or copy out the extracted.tgz for analysis. You may also use your standard computer forensic tools to copy/extract the extracted.tgz archive off your Encrypted Recovery USB drive.
14. Most of the relevant evidence in the extracted.tgz archive will be found within the “decrypted” folder. If there is only one user account on the Chromebox/Chromebook, that user account will be the “Owner” of the system. If there are multiple accounts present, the first created account will be the “Owner” of the system. For the “Owner” user, you will be interested in both the contents of the decrypted/mount and decrypted/encrypted folders. Most interesting user vault data will be found within decrypted/mount/user and system data will be found within the decrypted/encrypted folder. If the extracted user was NOT the system “Owner”, then the decrypted/encrypted folder, which would contain the decrypted contents of the encrypted.block file from the root of the stateful partition, will NOT be included in the decrypted backup and therefor no general system data is provided in your Encrypted Partition recovery.
15. The encrypted.tgz archive can be extracted and analyzed on your forensic workstation using your typical forensic tools of choice.



extracted.tgz\.\decrypted\mount\user\Downloads - TAR+GZIP archive, unpacked size 1,765,110,681 bytes

```
extracted.tgz
  .
    decrypted
      encrypted
        chronos
        lost+found
        var
      mount
        root
        user
          .pki
          .ssh
          Accounts
          arc.apps
          blob_storage
          BudgetDatabase
          Cache
          Code Cache
          data_reduction_prox
          databases
          Downloads
            Cats
            Dogs
          Extension Rules
          Extension State
```

Name	Size	Packed	Type	Modified
..			Local Disk	
Dogs			File folder	4/12/2019 6:51 AM
Cats			File folder	4/12/2019 6:51 AM
network_diagnostics_2019-04-10.08-14-32.txt	10,179	?	Text Document	4/12/2019 6:51 AM
2016-Ford-Mustang-Shelby-GT350-shelby-mustang-gt350...	86,406	?	JPG File	4/12/2019 6:51 AM

Total 2 folders and 96,585 bytes in 2 files

16. The Chromebook/Chromebox device has been left in the same operational state as when you started.

Important Lessons Learned and Limitations of the Encrypted Partition Recovery Process

Since the original release of this paper and process, forensic examiners around the world have been successfully acquiring decrypted data from seized Chromebook/Chromebox devices. However, through providing support and guidance to these examiners, some issues and limitation have come to light that everyone should be aware of.

1. All screenshots and splash screens in this go-by document were taken from a specific model Chromebook running a specific version/build of ChromeOS at the time in 2019. It has become evident that many Chromebook/Chromebox models and subsequent releases of newer the ChromeOS operating system come with different splash screens.

While it has been reported that many of the screens/graphics seen by forensic examiners on seized devices may not necessarily match the screenshots shown in my paper, the functionality and following the instructions at each step are the same and have not changed.

a. Pay attention to the recovery steps and not necessarily what splash screen you see. The wording on the screens may also vary slightly along with variations of the screen graphics.

2. Typing the correct username and password when prompted is critical to performing a successful Encrypted Partition Recovery.

a. The device will default to an American keyboard layout, where @ and “ are inverted. This is important for both email and password. Users should consider a "dry run" typing the password in the email field where the input can be previewed (e.g. passwords with @ and “ symbols). The password entry box doesn’t include * or any other output, so you have to be confident when typing the password as you cannot see the output of what you type, nor any typing mistakes.

b. As explained in the paper, Google does not use special characters in the prefix of Google (Gmail) email addresses, so you must type first.last@gmail.com as firstlast@gmail.com

c. However, Google/Chromebook accounts setup using a non-Gmail email address like first.last@hotmail.com may include special characters. So, if the recovery process fails when excluding the ".", you may need to retry the recovery using the entire original email address as-is.

3. This limitation is probably the MOST IMPORTANT! As explained earlier in this paper, Phase 1 of the Encrypted Partition Recovery process makes a temporary copy of the encrypted data ON THE AVAILABLE FREE SPACE of the internal storage of the Chromebook/Chromebox….unless/until the device runs out of free disk space in the process!

a. Each Chromebook/Chromebox has a specific amount of internal storage. Depending on how much data may be stored in the profile of each device user, there may be situations where there is NOT ENOUGH FREE SPACE to make a duplicate decrypted copy of all of the data on the internal storage during "Phase 1".

b. If the device runs out of free space while performing "Phase 1", it just stops when it runs out of space and continues to "Phase 2" to capture whatever it did copy before it ran out of free space.

c. If you have an advanced user that has turned on the Linux (Beta) functionality on their Chromebook/Chromebox device, this creates a rather large Linux Virtual Machine (VM) in the user's profile. This greatly increases the amount of data that has to be copied in the decryption "Phase 1" process and ma y run out of disk space in the process.

i. Even if the device has plenty of disk space, expect the copying and TGZ archiving of the large VM to take a while.

d. If a user's "Downloads" folder contains a large amount of data (files/folders), and the device has limited free space, then you may run into a situation where some of the contents of the "Downloads" folder is not included in the resulting extracted.tgz archive upon completion of a successful Encrypted Partition Recovery process because the device simply ran out of disk space.

e. Because of this limitation, it is now recommended that ALL examiners performing an Encrypted Partition Recovery process, ALSO do the following to ensure a most complete acquisition.

i. Boot the Chromebook/Chromebox and manually log into the user account at the GUI login screen.

ii. Using the “Files” application within ChromeOS, review the contents of the “MyFiles/Downloads” folder.

iii. Compare what you see in the “Downloads” folder with what was captured in the recovered extracted.tgz archive.

iv. If you see contents in “Downloads” that is NOT in the captured extracted.tgz archive, then you should MANUALLY copy all data from the live device’s “Downloads” folder onto a clean (wiped) USB formatted with an ExFAT filesystem.

v. This supplemental manual file/folder copy process is the only way to capture any data missing due to the Chromebook/Chromebox running out of disk space during “Phase 1” of the Encrypted Partition Recovery process.

4. On some model Chromebook/Chromebox devices, attempting to create an Encrypted Partition Recovery USB using a “spinning” disk in an external USB enclosure, rather than using a traditional flash USB device, has resulted in the device not invoking the recovery process. Recreating the Encrypted Partition Recovery USB on a regular flash storage USB device instead has corrected the problem and invoked the recovery process as expected.

In similar manner, on some Chromebook/Chromebox devices, it has been reported that invoking the Encrypted Partition Recovery process succeeded when using a microSD/SD storage card to create the Encrypted Partition Recover SD card, but did not invoke trying to use a standard USB device created as an Encrypted Partition Recovery USB.

5. If your device has multiple accounts and you wish to perform a decrypted recovery for each account, you essentially just repeat the exact same recovery process for each account and the only difference is which user account you provide the username/password for during the process.

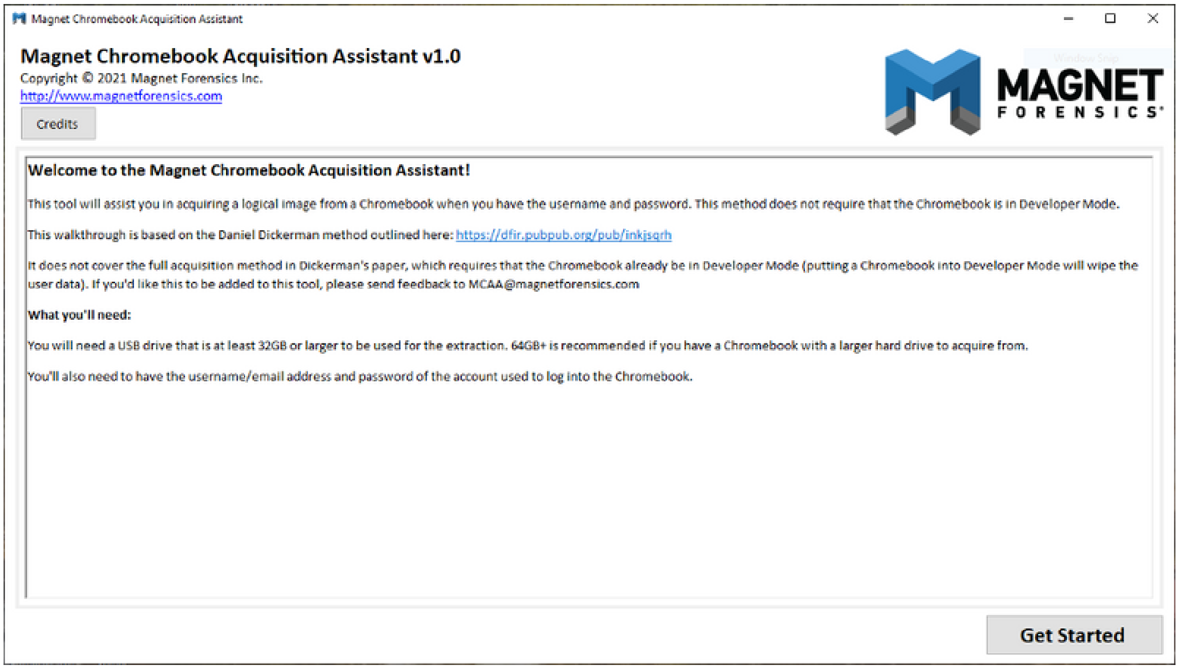
a. If you do multiple extractions, make sure you copy off or otherwise preserve the captured data (extracted.tgz file) after each capture so you don’t overwrite one extracted.tgz extraction with your next extraction having the same extracted.tgz filename.

New Tool: Magnet Chromebook Acquisition Assistant v1.0

I am excited to announce that as I had hoped, this paper and work has prompted industry response to improve this process and make it easier for the forensic examiner.

On February 25, 2021, Magnet Forensics, through their Idea Lab, has released an easy-to-use wizard tool that greatly simplifies the building of your Encrypted Partition Recovery USBs. This tool allows you to create the needed Encrypted Partition Recovery USB without needing to create and use a ChromiumOS USB and without needing to perform an *unix command-line commands to run the scripts that build the USBs.

As explained in the information in the tool, you must still read through all of the sections of this paper to fully understand the recovery process before you attempt any recovery using USBs created by this tool or using the manual build process.



Magnet Chromebook Acquisition Assistant v1.0

Copyright © 2021 Magnet Forensics Inc.

http://www.magnetforensics.com

Welcome to the Magnet Chromebook Acquisition Assistant!

This tool will assist you in acquiring a logical image from a Chromebook when you have the username and password. This method does not require that the Chromebook is in Developer Mode.

This walkthrough is based on the Daniel Dickerman method outlined here: https://dfir.pubpub.org/pub/inkjsqrh

It does not cover the full acquisition method in Dickerman's paper, which requires that the Chromebook already be in Developer Mode (putting a Chromebook into Developer Mode will wipe the user data). If you'd like this to be added to this tool, please send feedback to MCAA@magnetforensics.com

What you'll need:

You will need a USB drive that is at least 32GB or larger to be used for the extraction. 64GB+ is recommended if you have a Chromebook with a larger hard drive to acquire from.

You'll also need to have the username/email address and password of the account used to log into the Chromebook.

Thank you to Magnet for this outstanding contribution to the forensic industry and this work!

The direct link to the tool is here: https://magnetidealab.com/chromebook-aa/

Capturing a Full Physical Disk Clone

Note: Prior to performing any steps in the section, make sure you have served legal process to Google, as explained at the beginning of this document, to obtain all stored *cloud data for any accounts used on the seized Chromebook or Chromebox device.*

The procedure in this section produces a complete raw bitstream physical disk clone of a seized Chromebook's internal HD. In order to accomplish this, the Chromebook must be in Developer Mode. If the Chromebook is already in Developer Mode, these procedures produce a physical clone of the Chromebook's internal HD and leaves the existing Chromebook in the same state it was in before cloning the Chromebook. Examiners with advanced Linux skills may choose to perform their own data acquisition with dd or other tools. The script and instructions provided in this section are to provide an automated cloning acquisition process for users that are not Linux savvy.

If the Chromebook was not already in Developer Mode and you attempt to switch the Chromebook/Chromebox into Developer Mode, you will clear the TPM in the process and render all encrypted data unrecoverable. DO NOT switch device to Developer Mode, making it impossible to perform an Encrypted Partition recovery as described in the previous section of this document. If you switch to Developer Mode all user accounts will be cleared and you will be presented with an "Out Of the Box Experience" (OOBE) requiring the setup of new accounts.

User data on the Chromebook's internal HD is stored within each user's encrypted folder structure located in /mnt/stateful_partition/home/.shadow/. These folders are located on partition 1 of the internal HD, which is an ext4 partition (i.e. /dev/mmcblk0p1).

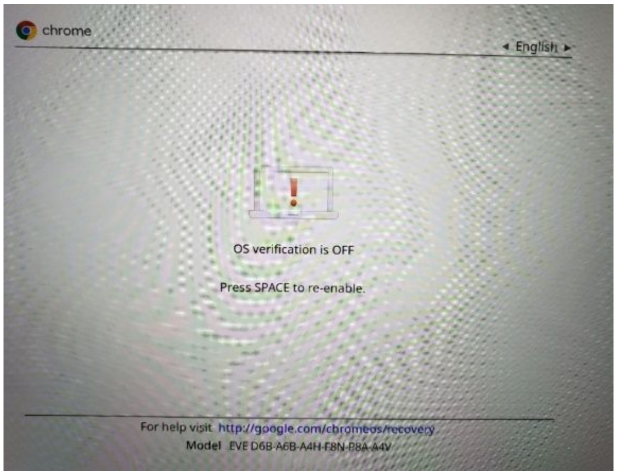
Pulling the Hard Drive

While not covered in detail in this document, physically pulling the hard drive from a Chromebook/Chromebox and obtaining a physical image or clone may be an option to consider for devices in "Normal Mode." Make sure you put the drive back in and leave the device in Normal Mode, in the same state as it was when you received it if you want any future possibility of performing an Encrypted Partition Recovery or otherwise log into any existing accounts on the device.

Cloning a Device Already in Developer Mode

1. Read all steps in this section in their entirety before you go through this process! There are certain steps that MUST be followed EXACTLY as explained!
2. If the Chromebook/Chromebox was ALREADY in Developer Mode when you received it, you should see the following screen upon powering on the

Chromebook/Chromebox device. At his screen, press CTRL+D to boot the native ChromeOS.



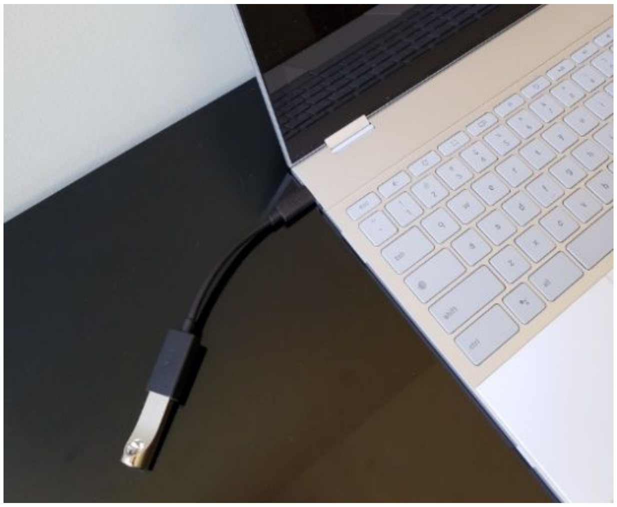
OS verification is OFF

Press SPACE to re-enable.

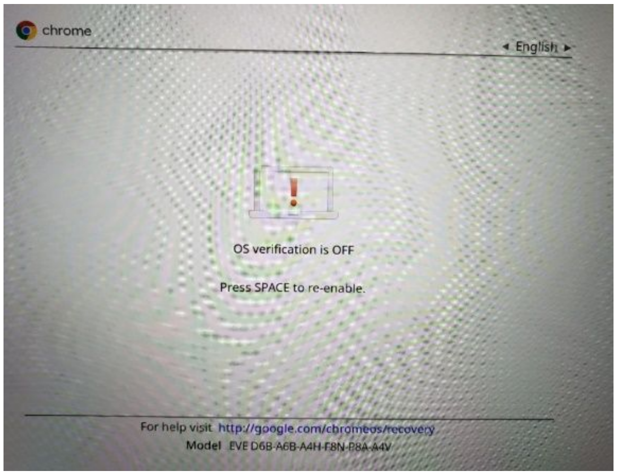
For help visit http://google.com/chromeos/recovery

Model EVE D6B-A6B-A4H-F8N-P8A-A4V

3. At the native ChromeOS login screen, where existing user accounts are presented to you, press CTRL+ALT+F2 to switch to a virtual terminal (TTY1). Log on as the user ‘root’ with no password required.
4. To ensure that booting from your Chromium OS live USB drive is allowed, at the root prompt, type “crossystem dev_boot_legacy=1 dev_boot_usb=1” without the quotes and hit enter.
5. Note that for *nix-savvy users, you have full root access right now and may choose to image using dd however you wish, perform searching or triage, capture RAM, or perform any other desired task. The following steps are for non-*nix-savvy users that need a simple method for cloning the internal Chromebook/Chromebox hard drive.
6. Press CTRL+ALT+F1 to switch back to the GUI login screen and shutdown the device normally.
7. Attach your Chromium OS live USB drive and power on the Chromebook, then at the Developer Mode startup screen (screen says “OS verification is OFF”), press CTLR+U to boot into Chromium OS. Make sure no other USB drives are attached yet!



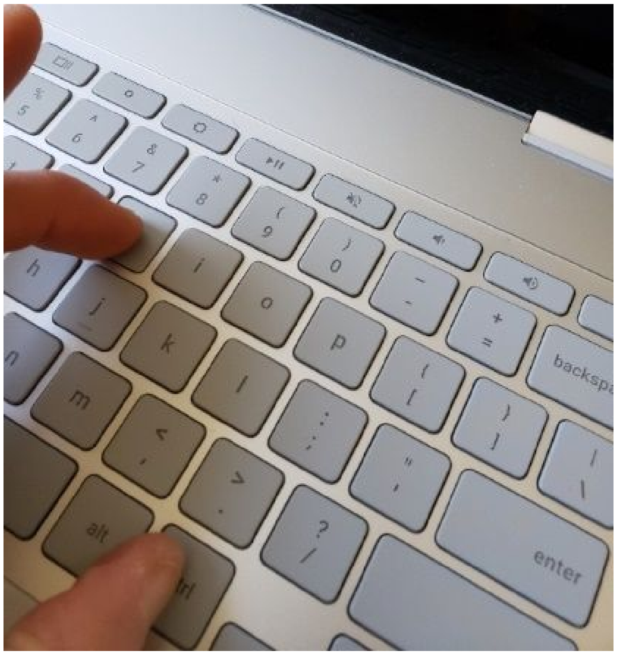
>



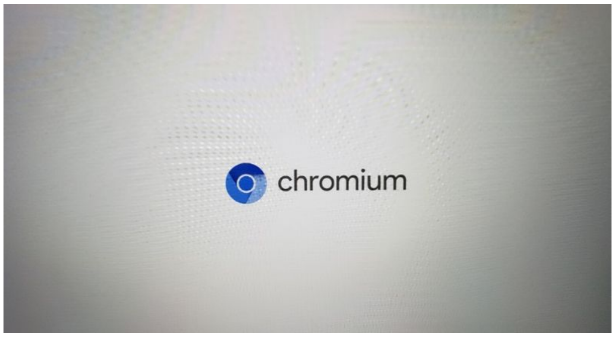
OS verification is OFF

Press SPACE to re-enable.

For help visit http://google.com/chromeos/recovery
Model EVE D6B-A6B-A4H-F8N-P8A-A4V



>



8. Once booted to your Chromium OS live USB, at the initial startup Splash Screen, press CTRL+ALT+F2 to switch to a virtual terminal (TTY1). Log on as the user ‘root’ with no password required.
9. Attach your previously prepared clone output destination USB drive, using the procedures discussed earlier in this document. Make sure the Chromebook is plugged in and providing enough power for destination drive and the Chromebook for the duration of the cloning process.
10. Run the script to clone the internal Chromebook/Chromebox hard drive to the attached prepared destination USB drive, using the command: “. /home/scripts/image_chromebook.sh” without the quotes. Make sure you have a space between the ‘.’ and /home/scripts/image_chromebook.sh.
11. Wait until the dd cloning process is complete. Progress and imaging speed will be displayed on your screen. If your screen goes to sleep you may hit “Esc” to wake the

screen back up.

12. Exit out of the logged in TTY1 shell by typing “exit” and hitting enter.
13. Switch back to the GUI splash screen by pressing CTRL+ALT+F1. Shutdown Chromium by clicking on the Shut Down icon in the lower left corner of the Splash Screen.
14. You may now remove the Chromium OS live USB and your newly cloned destination USB device.
15. The Chromebook/Chromebox has been left in the same operational state as when you started.

Analysis and Beyond...

You now have either decrypted user and/or system data from an Encrypted Partition Recovery, or a forensic image or clone of the internal Chromebook HD from the above scripts, from pulling the hard drive out of a Chromebook/Chromebox that is in “normal mode”, or your own physical acquisition process. You have a variety of both unencrypted and encrypted data available and may use the forensic tools of your choice to parse, search, carve, etc.

Triage of an Encrypted Chromebook Hard Drive

The triage script provided for this section may be of use when you ONLY have an encrypted original hard drive or clone from a Chromebook/Chromebox. The triage_stateful.sh script allows an examiner to quickly see if the Chromebook/Chromebox user(s) has files and/or folders in their “Downloads” folder. Although the data is encrypted, using file system metadata we are able to identify the Downloads folder for each encrypted user vault on the hard drive and enumerate the contents of the Downloads folder(s).

1. Boot any non-Chromebook (non-evidence) computer to your Chromium OS live USB.
2. Once booted to your Chromium OS live USB, at the initial startup Splash Screen, press CTRL+ALT+F2 to switch to a virtual terminal (TTY1). Log on as the user ‘root’ with no password required.
3. Attach, via USB, the Chromebook/Chromebox hard drive or clone containing encrypted user vaults (located in /home/.shadow of the STATE partition of the drive).
4. The run the bash script to triage the user(s) encrypted vaults on the attached hard drive, using the command: “. /home/scripts/triage_stateful.sh” without the quotes. Make sure you have a space between the ‘.’ and /home/scripts/triage_stateful.sh. Follow the prompts.

5. You will be prompted to enter any known username (i.e. email address) of any user accounts that were used on this Chromebook/Chromebox?
    1. Type each of the known username(s) separated by a space and hit ENTER. Type VERY carefully because there is no backspace or delete in this script.
    2. Goggle does not use special characters in the prefix of email addresses, so you must type first.last@gmail.com as firstlast@gmail.com!
6. The script will tell you which encrypted vault belongs to any usernames you provide.
7. The script will enumerate the contents of the Downloads folder of each encrypted vault.

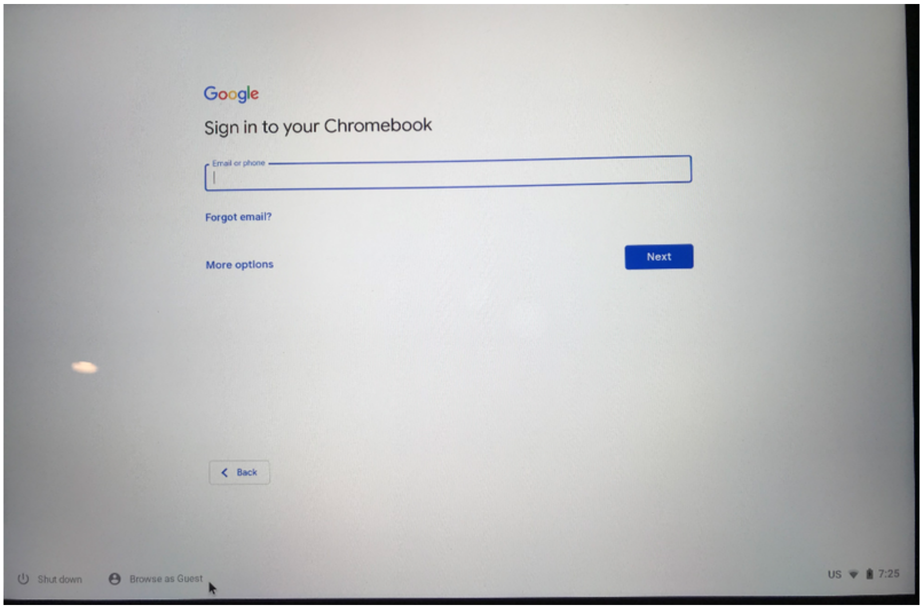
Live GUI Analysis for General System Information

Additionally, booting into the native ChromeOS will allow you to use the Chrome Browser in the ChromeOS GUI environment to access chrome://chrome-urls/. These URLS provide a vast amount of information about the Chromebook, so you will want to explore and document as desired. The below URL and other online resources will provide you further information about the available information.

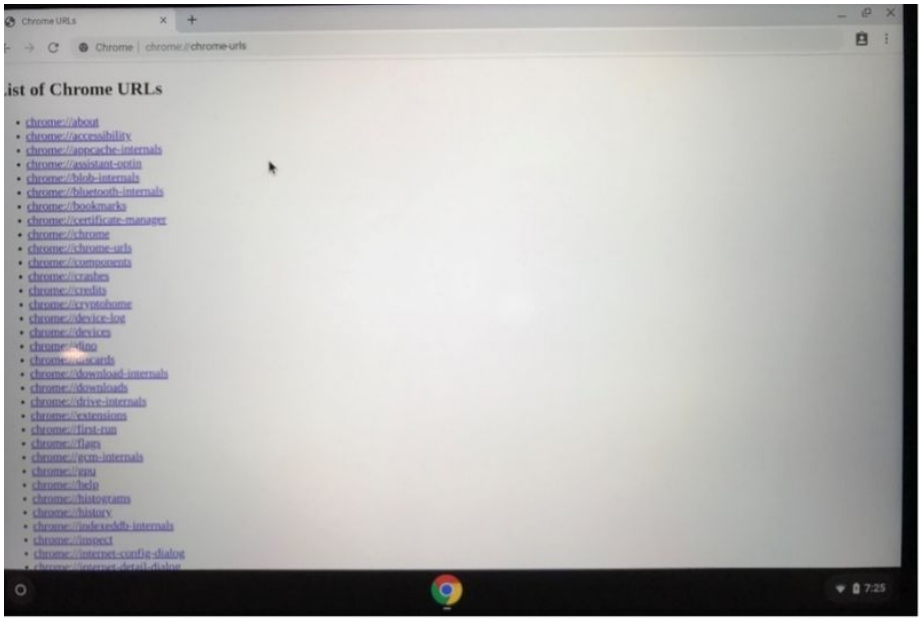
https://www.ghacks.net/2012/09/04/list-of-chrome-urls-and-their-purpose/

To access chrome://chrome-urls/, do the following:

1. At the GUI login screen, you will click on the "Browse as Guest" button in the lower left corner of the screen.



2. Open the Chrome Browser, if it doesn't automatically open, and enter chrome://chrome-urls/ in the Chrome address bar. Now explore the many links.



List of Chrome URLs

- chrome://about
- chrome://accessibility
- chrome://appcache-internals
- chrome://assistant-optin
- chrome://blob-internals
- chrome://bluetooth-internals
- chrome://bookmarks
- chrome://certificate-manager
- chrome://chrome
- chrome://chrome-urls
- chrome://components
- chrome://crashes
- chrome://credits
- chrome://cryptohome
- chrome://device-log
- chrome://devices
- chrome://dino
- chrome://discards
- chrome://download-internals
- chrome://downloads
- chrome://drive-internals
- chrome://extensions
- chrome://first-run
- chrome://flags
- chrome://gcm-internals
- chrome://gpu
- chrome://help
- chrome://histograms
- chrome://history
- chrome://indexeddb-internals
- chrome://inspect
- chrome://internet-config-dialog
- chrome://internet-detail-dialog

3. Once in the Chrome Browser, you can also press CTRL+ALT+T to open a terminal window within the Chrome Browser. The help and help_advanced commands will provide you much information at the crosh> prompt. Many of the available commands will provide information you may be interested in. If the Chromebook/Chromebox is in Developer mode, you can additionally type "shell" and hit enter to get a full root shell in the terminal window within the Chrome Browser.

Future Work...

This "Analysis and beyond..." section of this whitepaper is just a quick set of instructions to get you started. This is an in-depth work in progress and future revisions of this document will provide further information on the forensic analysis of Chromebooks.

Any contributions from other researchers on Chromebook analysis and artifacts is welcome and encouraged.

Attachments: Bash Scripts

zip public release scripts v1.2.zip 16 KB

DFIR Review

This paper provides a step-by-step guide for acquiring evidence from a Chromebook. This is particularly useful due to the limited amount of prior literature in this area. This paper was also peer-reviewed as part of the VTO Brews and Bytes event that took place in Denver, Colorado on November 11, 2019. The directions provided in the paper were used to acquire evidence from three devices (Samsung Gen 3 XE501C13, Asus C100PA Flip, Lenovo C330 H1HY). One reviewer noted that they were unsuccessful with acquiring at least one type of device. Another reviewer found that it may not be necessary to have three USB drives, a device with a capacity of 32 GB or higher that can make a USB connection can be used. They were able to create live and recovery USBs using a 2TB external hard drive, which may also provide greater speed than USB flash drives.

The updated version of this paper was reviewed. The reviewers found that the updated version includes helpful notes and clarifications. The updates to the paper add clarity and make it easier to follow. One of the reviewers tested the "Encrypted Partition Recovery" portion of this work and found that it worked on one test device, multiple times. This work and acquisition method is of great benefit to the digital forensics community.

Future Work

Further research in troubleshooting the bash scripts with the ChromeOS Recovery images for various models and builds would be helpful. It may also be interesting to see this logical-style extraction of individual user accounts performed repeatedly to see if there are any differences between successive acquisitions.

This extraction could also be performed on a Chromebook with developer mode enabled. If a physical image of the drive was taken before and after the acquisition, the artifacts left behind (if any) by this type of extraction could be enumerated so investigators are better able to explain the ramifications of their actions.

Future work could also include validation on generic Chromebook systems (i.e. non-Chromebook computers that have the open source Chromium OS installed on them)

Reviewers

- Jessica Hyde (Methodology Review, Validated Review using Reviewer Generated Datasets)

- Timothy Bollé (Methodology Review)
- Linda Shou (Methodology Review, Validated Review using Reviewer Generated Datasets)
- Lisa Brown (Methodology Review)